

# On Abelianized Absolute Galois Group of Global Function Fields

Bart de Smit

`desmit@math.leidenuniv.nl`<sup>\*</sup> and

Pavel Solomatin

`p.solomatin@math.leidenuniv.nl`<sup>\*</sup>

<sup>\*</sup>Leiden University, Mathematical Department, Niels Bohrweg 1, 2333  
CA Leiden

Leiden, 2017

## Abstract

The main purpose of this paper is to describe the abelian part  $\mathcal{G}_K^{ab}$  of the absolute Galois group of a global function field  $K$  as pro-finite group. We will show that the characteristic  $p$  of  $K$  and the non  $p$ -part of the class group of  $K$  are determined by  $\mathcal{G}_K^{ab}$ . The converse is almost true: isomorphism type of  $\mathcal{G}_K^{ab}$  as pro-finite group is determined by the invariant  $d_K$  of the constant field  $\mathbb{F}_q$  introduced in first section and the non  $p$ -part of the class group.

**Acknowledgements:** This paper is a part of the PhD research of the second author under scientific direction of the first author. The second author was supported by the ALGANT scholarship during this research. Both authors would like to thank professors Hendrick Lenstra and Peter Stevenhagen for helpful discussions during the project.

# 1 Introduction

Let  $K$  be a global function field, i.e. field of functions on a smooth projective geometrically connected curve  $X$  defined over a finite field  $\mathbb{F}_q$ , where  $q = p^n$ ,  $p$  is prime. The famous theorem of Uchida [11] states that the geometric isomorphism class of  $X$  is determined by the isomorphism class of the absolute Galois group  $\mathcal{G}_K = \text{Gal}(K^{sep} : K)$  considered as topological group. One of the essential step in the Uchida's proof is to recover from  $\mathcal{G}_K$  its abelian part  $\mathcal{G}_K^{ab}$  with some additional data, like decomposition and inertia subgroups. The following questions are natural to ask: what kind of information one could recover from the isomorphism class of the pro-finite abelian group  $\mathcal{G}_K^{ab}$ ? More concretely, does the abelian part of the absolute Galois group determine the global function field  $K$  up to isomorphism? If not which function fields share the same  $\mathcal{G}_K^{ab}$  for some fixed isomorphism class of  $\mathcal{G}_K^{ab}$ ?

For a global function field  $K$  of characteristic  $p$  with the exact constant field  $\mathbb{F}_q$ ,  $q = p^n$  we define the invariant  $d_K$  as a natural number such that  $n = p^k d_K$  with  $\gcd(d_K, p) = 1$ . Let  $\text{Cl}^0(K)$  denotes the degree zero part of the class-group of  $K$ . In other words  $\text{Cl}^0(K)$  is the abelian group of  $\mathbb{F}_q$ -rational points of the Jacobian variety associated to the curve  $X$ . The main purpose of this paper is to prove the following result:

**Theorem 1.** *Suppose  $K$  and  $K'$  are two global function fields, then  $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$  as pro-finite groups if and only if the following three conditions hold:*

1.  $K$  and  $K'$  share the same characteristic  $p$ ;
2. Invariants  $d_K$  and  $d_{K'}$  coincide:  $d_K = d_{K'}$ ;
3. The non  $p$ -parts of class-groups of  $K$  and  $K'$  are isomorphic:

$$\text{Cl}_{non-p}^0(K) \simeq \text{Cl}_{non-p}^0(K').$$

*In particular, two function fields with the same exact constant field  $\mathbb{F}_q$  have isomorphic  $\mathcal{G}_K^{ab}$  if and only if they have isomorphic  $\text{Cl}_{non-p}^0(K)$ .*

This theorem provides some answers to the above questions. For example, we have:

**Corollary 1.** *Let  $K$  be the rational function field (with genus zero) over fixed constant field  $\mathbb{F}_q$  and let  $E$  be an elliptic function field (with genus one) defined over the same constant field, such that<sup>1</sup>  $\# \text{Cl}^0(E) = q$ . Then there exists isomorphism of topological groups  $\mathcal{G}_K^{ab} \simeq \mathcal{G}_E^{ab}$ . In particular, the genus  $g$  of  $K$  and therefore the Dedekind zeta-function  $\zeta_K(s)$  of  $K$  are not determined by  $\mathcal{G}_K^{ab}$  even if the constant field  $\mathbb{F}_q$  is fixed.*

---

<sup>1</sup>the existence of such field is guaranteed by the Waterhouse theorem, see the last section.

The above example also shows that:

**Corollary 2.** *There are infinitely many function fields of the same characteristic  $p$  (but with different cardinality of the constant field) with isomorphic  $\mathcal{G}_K^{ab}$ .*

*Proof.* Fix a prime number  $p$  and let  $q = p^{p^k}$ , where  $k$  is a non-negative integer. Let  $F_k$  and  $E_k$  denote rational and elliptic function fields from the previous example with the exact constant field  $\mathbb{F}_q$ . Then, according to the our main theorem for any non-negative integers  $k, l$  we have:  $\mathcal{G}_{K_l}^{ab} \simeq \mathcal{G}_{E_k}^{ab}$ .  $\square$

Applying some classical results about the two-part of  $\text{Cl}^0(K)$  of hyper-elliptic function fields we will also show that:

**Corollary 3.** *For any given  $q$  with  $p > 2$  there are infinitely many isomorphism types of  $\mathcal{G}_K^{ab}$  which could occur for function fields with the exact constant field  $\mathbb{F}_q$ .*

*Proof.* See theorem 10 from the last section.  $\square$

Unfortunately, the answer to the question about distribution of global fields over fixed constant field  $\mathbb{F}_q$  sharing the same  $\mathcal{G}_K^{ab}$  is not clear at the moment, since we don't know if there are infinitely many such fields with a given non  $p$ -part of the class group. In particular, it seems to be reasonable to state the following **conjecture**: *there are infinitely many curves defined over fixed finite field  $\mathbb{F}_q$ ,  $q = p^n$  with the order of the group of  $\mathbb{F}_q$ -rational points of the Jacobian varieties associated to them to be a power of  $p$ .* If the conjecture is true then what is the proportion of such curves, say as  $q$  fixed and  $g$  tends to infinity?

Note that the proof of the theorem 1 includes the explicit reconstruction of the invariants  $p, d_K$  and  $\text{Cl}_{non-p}^0(K)$  from  $\mathcal{G}_K^{ab}$ . More concretely, let  $s_l(\mathcal{G}_K^{ab})$  be the least integer  $k$  such that  $\mathcal{G}_K^{ab}$  has direct summand of the form  $\mathbb{Z}/l^k\mathbb{Z}$  and let  $p^*$  denotes  $(-1)^{\frac{p-1}{2}}p$  if  $p$  is odd and  $p$  otherwise, then:

**Theorem 2.** *Given the isomorphism class of the topological group  $\mathcal{G}_K^{ab}$  we have:*

1. *The characteristic  $p$  of  $K$  is a unique prime such  $\mathcal{G}_K^{ab}$  has no elements of order  $p$ ;*
2. *The non- $p$  part  $\text{Cl}_{non-p}^0(K)$  of the class-groups of  $K$  is isomorphic to the torsion of the quotient  $\mathcal{G}_K^{ab}/\overline{\mathcal{G}_K^{ab}[\text{tors}]}$ , where  $\overline{\mathcal{G}_K^{ab}[\text{tors}]}$  denotes the closure of the torsion subgroup of  $\mathcal{G}_K^{ab}$  :*

$$\text{Cl}_{non-p}^0(K) \simeq (\mathcal{G}_K^{ab}/\overline{\mathcal{G}_K^{ab}[\text{tors}]})[\text{tors}].$$

3. The natural number  $d_K$  is a unique number such that for any prime number  $l \neq p$ :

$$\text{ord}_l(d_K) = \begin{cases} 0, & \text{if } l = 2 \text{ and } s_2(\mathcal{G}_K^{ab}) = 1; \\ s_l(\mathcal{G}_K^{ab}) - \text{ord}_l((p^*)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

*Proof.* See corollaries 4 and 5. □

The main idea towards our result was inspired by the work [1], where authors produced an elegant description for isomorphism class of the topological group  $\mathcal{G}_K^{ab}$ , where  $K$  denotes *imaginary quadratic number field*. But also, note that there are many completely different technical details, which give in some sense opposite to their result.

The paper has the following structure: in the next section we will sketch the proof of the theorem 1. Then we prove all the necessarily lemmas. Finally, we will discuss the question about construction of non-isomorphic function fields with isomorphic and non-isomorphic abelian parts of their absolute Galois groups.

## 2 Outline of the Proof

The global class field theory provides an inherits description of the abelian part of the absolute Galois group of a global or local field  $K$  in terms of different arithmetic objects associated to  $K$ . We will use the *Idele*-theoretical approach, see section 3.2 for details and the following classical books [8], [12], [2] for complete discussion. For a given global function field  $K$  with the exact constant field  $\mathbb{F}_q$ ,  $q = p^n$ ,  $p$  is prime let  $\mathcal{I}_K$  denotes the group of Ideles of  $K$  and  $\mathcal{C}_K$  denotes the *Idele class-group* of  $K$ , i.e. the quotient group of  $\mathcal{I}_K$  by the multiplicative group  $K^\times$ . Then the Artin map provides us with the homomorphism  $\mathcal{C}_K \rightarrow \mathcal{G}_K^{ab}$ . In the function field case this map is injective, but not surjective, since  $\mathcal{C}_K$  is not compact. But if we take the pro-finite completion (with respect to the given topology) of  $\mathcal{C}_K$  then the main theorem of the class field theory says that we have isomorphism of topological groups:  $\widehat{\mathcal{C}_K} \simeq \mathcal{G}_K^{ab}$ , see for example [theorem 6, chapter 9 of [12]].

Recall that we have a split exact sequence:

$$0 \rightarrow \mathcal{C}_K^0 \rightarrow \mathcal{C}_K \rightarrow \mathbb{Z} \rightarrow 0,$$

where  $\mathcal{C}_K^0$  is the degree zero part of the Idele class group and the map from  $\mathcal{C}_K$  to  $\mathbb{Z}$  is the degree map. Now,  $\mathcal{C}_K^0$  is pro-finite, hence complete and therefore  $\widehat{\mathcal{C}_K} \simeq \mathcal{C}_K^0 \oplus \widehat{\mathbb{Z}}$ . We will show that  $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$  if and only if  $\mathcal{C}_K^0 \simeq \mathcal{C}_{K'}^0$ . The key ingredient in the our proof is the Pontryagin duality for locally compact abelian groups, which allows us to reduce question about pro-finite abelian groups to the question about discrete torsion groups.

**Lemma 1.** *Let  $A$  and  $B$  be two pro-finite abelian groups. Then  $A \simeq B$  if and only if  $A \oplus \widehat{\mathbb{Z}} \simeq B \oplus \widehat{\mathbb{Z}}$  in the category of pro-finite abelian groups.*

*Proof.* See section 3.1.1. □

This lemma reduces our question to the description of  $\mathcal{C}_K^0$  as topological group. Let  $v$  denotes a place of  $K$  and  $K_v$ ,  $\mathcal{O}_v$  denotes the corresponding completion and its ring of integers respectively. Then we derive the following exact sequence.

**Lemma 2.** *There exists an exact sequence of topological groups, where all finite groups treated with the discrete topology:*

$$1 \rightarrow \mathbb{F}_q^\times \rightarrow \prod_v \mathcal{O}_v^\times \rightarrow \mathcal{C}_K^0 \rightarrow \text{Cl}^0(K) \rightarrow 1.$$

*Proof.* See section 3.3. □

After that we recall the isomorphism  $\mathcal{O}_v^\times \simeq \mathbb{F}_{q^n}^\times \times \mathbb{Z}_p^\infty$ , where  $n$  is the degree of a place  $v$  and  $\mathbb{Z}_p$  denotes the group of  $p$ -adic integers. Denoting by  $\mathcal{T}_K$  the group  $(\prod_v \mathbb{F}_{q^{\deg(v)}}^\times) / \mathbb{F}_q^\times$  we will get the following exact sequence:

$$1 \rightarrow \mathcal{T}_K \times \mathbb{Z}_p^\infty \rightarrow \mathcal{C}_K^0 \rightarrow \text{Cl}^0(K) \rightarrow 1 \quad (1)$$

There are two crucial observation about this sequence. First we will prove the following structure theorem for the group  $\mathcal{T}_K$ :

**Theorem 3.** *Given a function field  $K$  with the exact constant field  $\mathbb{F}_q$ , where  $q = p^n$  there exists an isomorphism  $\mathcal{T}_K \simeq \prod_{l,m} (\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}}$ , where the product is taken over all prime numbers  $l$  and all positive integers  $m$  and  $a_{l,m}$  denotes a finite or countable cardinal number. Moreover, coefficients  $a_{l,m}$  depend only on  $q$  and the following holds:*

1. *Each  $a_{l,m}$  is either zero or infinite countable cardinal;*
2. *For  $l = p$  we have  $a_{p,m} = 0$  for all  $m$ ;*
3. *For  $l \neq p$ ,  $l \neq 2$  there exists a unique non-negative integer  $N_q(l)$  such that  $a_{l,m}$  is infinite if and only if  $m \geq N_q(l)$ ;*
4. *For  $p \neq 2$  and  $l = 2$  there exists a unique non-negative integer  $N_q(2)$  such that for  $q \equiv 1 \pmod{4}$  we have  $a_{2,m}$  is infinite if and only if  $m \geq N_q(2)$ , and for  $q \equiv 3 \pmod{4}$  we have  $a_{2,m}$  is infinite if and only if  $m = 1$  or  $m \geq N_q(2)$ ;*

5. Given two prime powers  $q_1, q_2$  numbers  $N_{q_1}(l)$  and  $N_{q_2}(l)$  coincide for all  $l$  if and only if  $q_1 = p^{n_1}, q_2 = p^{n_2}$  with  $\frac{n_1}{n_2} = p^m$ , for some integer  $m$ .

*Proof.* See section 3.4.1. □

From now we denote the group  $\mathcal{T}_K$  by  $\mathcal{T}_q$ .

**Definition 1.** The exact sequence of abelian groups  $0 \rightarrow A \rightarrow B \rightarrow^\psi C \rightarrow 0$  is called totally non-split if there is no non-trivial subgroup  $S$  of  $C$  such that the sequence  $0 \rightarrow A \rightarrow \psi^{-1}(S) \rightarrow S \rightarrow 0$  splits.

The second observation is the key point in the our proof.

**Theorem 4.** All torsion elements of  $\mathcal{C}_K^0$  are in  $\mathcal{T}_q$ . Therefore the exact sequence 1 is totally non-split. Moreover, the topological closure of the torsion subgroup of  $\mathcal{C}_K^0$  is  $\mathcal{T}_q : \mathcal{C}_K^0[\text{tors}] = \mathcal{T}_q$ .

*Proof.* See section 3.5. □

Because of the description of  $\mathcal{T}_q$  this theorem gives us:

**Corollary 4.** If  $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$  as pro-finite groups then  $K$  and  $K'$  share the same group  $\mathcal{T}_q$ , in particular the characteristic  $p$  and the invariant  $d_K$  are determined by the isomorphism class of  $\mathcal{G}_K^{ab}$ .

*Proof.* Since  $\mathcal{G}_K^{ab} \simeq \mathcal{C}_K^0 \oplus \widehat{\mathbb{Z}}$  and the group  $\widehat{\mathbb{Z}}$  is torsion free, we have that  $\mathcal{T}_q$  is also the closure of the torsion subgroup of  $\mathcal{G}_K^{ab}$ . Then theorem 3 shows that  $p$  is a unique prime such that this group has no elements of order  $p$ .

For the natural number  $d_K$  consider the torsion group  $\mathcal{G}_K^{ab}[\text{tors}]$ . By the theorem 3 this group has direct summand of the form  $\mathbb{Z}/l^k\mathbb{Z}$  for a fixed prime  $l \neq p$  if and only if  $k \geq N_q(l)$  or  $l = 2, k = 1, p = 3 \pmod{4}$  and  $d_K = 1 \pmod{2}$ . In the proof of the theorem 3 we will show that  $N_q(l) = \text{ord}_l(d_K) + \text{ord}_l((p^*)^{l-1} - 1)$ , where  $p^* = -p$  if  $p = 3 \pmod{4}$  and  $p^* = p$  otherwise. Which implies the formula:

$$\text{ord}_l(d_K) = \begin{cases} 0, & \text{if } l = 2 \text{ and } s_2 = 1 \\ s_l(\mathcal{G}_K^{ab}) - \text{ord}_l((p^*)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

□

Since each pro-finite abelian group is isomorphic to the limit of finite abelian groups, by the Chinese remainder theorem it is also isomorphic to the product over prime numbers of its primary components. We will work with these components separately instead of working with the whole group. Let  $l$  be a prime number different from  $p$ , we have:  $1 \rightarrow \mathcal{T}_{q,l} \rightarrow \mathcal{C}_{K,l}^0 \rightarrow \text{Cl}_l^0(K) \rightarrow 1$ . Which shows that:

$$\text{Cl}_l^0(K) \simeq \mathcal{C}_{K,l}^0 / \overline{\mathcal{C}_{K,l}^0[\text{tors}]}$$

**Corollary 5.** *If  $\mathcal{G}_K^{ab} \simeq \mathcal{G}_{K'}^{ab}$  as pro-finite groups then the non  $p$ -parts of the class-groups of  $K$  and  $K'$  are isomorphic:  $\text{Cl}_{\text{non-}p}^0(K) \simeq \text{Cl}_{\text{non-}p}^0(K')$ .*

*Proof.* We know that  $\mathcal{G}_K^{ab} \simeq \mathcal{C}_K^0 \oplus \widehat{\mathbb{Z}}$  and that  $\mathcal{T}_q = \overline{\mathcal{G}_K^{ab}[\text{tors}]}$ . Considering the  $l$ -part we get:

$$\mathcal{G}_{K,l}^{ab} / \overline{\mathcal{G}_{K,l}^{ab}[\text{tors}]} \simeq (\mathcal{C}_{K,l}^0 / \mathcal{T}_{q,l}) \oplus \mathbb{Z}_l.$$

Since  $\mathbb{Z}_l$  is torsion free, we have:

$$(\mathcal{G}_{K,l}^{ab} / \overline{\mathcal{G}_{K,l}^{ab}[\text{tors}]})[\text{tors}] \simeq \mathcal{C}_{K,l}^0 / \mathcal{T}_{q,l} \simeq \text{Cl}_l^0(K).$$

Finally, note that the  $p$ -part of the torsion group of  $\mathcal{G}_K^{ab}$  is trivial and hence combining all primes  $l$  different from  $p$  we get:

$$\text{Cl}_{\text{non-}p}^0(K) \simeq (\mathcal{G}_K^{ab} / \overline{\mathcal{G}_K^{ab}[\text{tors}]})[\text{tors}].$$

□

These two results imply the only if part of the theorem 1. Now, we are going to discuss the question about the other implication. Our goal is to show that for a given  $\mathcal{T}_q$  and given non  $p$ -part of the class group there is only one possibility for  $\mathcal{C}_K^0$  to fit in the exact sequence 1.

Consider the  $p$ -part of the exact sequence 1:

$$1 \rightarrow \mathbb{Z}_p^\infty \rightarrow \mathcal{C}_{K,p}^0 \rightarrow \text{Cl}_p^0(K) \rightarrow 1.$$

By using the fact that this sequence is totally non-split we will show (see lemma 13) that this implies  $\mathcal{C}_{K,p}^0 \simeq \mathbb{Z}_p^\infty$ , in particular  $\mathcal{G}_{K,p}^{ab}$  doesn't depend on  $\text{Cl}_p^0(K)$ .

We fix a prime number  $l \neq p$  and consider the  $l$ -part which is of course also totally non-split:

$$1 \rightarrow \mathcal{T}_{q,l} \rightarrow \mathcal{C}_{K,l}^0 \rightarrow \text{Cl}_l^0(K) \rightarrow 1 \tag{2}$$

Obviously, if  $\text{Cl}_l^0(K) \simeq 0$  then  $\mathcal{C}_{K,l}^0 \simeq \mathcal{T}_{q,l}$ . Our goal is to show that even if  $\text{Cl}_l^0(K)$  is not the trivial group then this totally non-split sequence determines  $\mathcal{C}_{K,l}^0$  uniquely. In order to achieve our goal we need the following:

**Theorem 5.** *Let  $\{C_i\}$  be a countable set of finite cyclic abelian  $l$ -groups with orders of  $C_i$  are not bounded as  $i$  tends to infinity and let  $A$  be any finite abelian  $l$ -group. Then up to isomorphism there exists and unique torsion abelian  $l$ -group  $B$  satisfying two following conditions:*

1. *There exists an exact sequence:  $1 \rightarrow A \rightarrow B \rightarrow \oplus_{i \geq 1} C_i \rightarrow 1$ ;*
2.  *$A$  is the union of all divisible elements of  $B$ :  $A = \cap_{n \geq 1} nB$ .*

Applying the Pontryagin duality to the exact sequence 2 we get:

$$1 \leftarrow (\mathcal{T}_{q,l})^\vee \leftarrow (\mathcal{C}_{K,l}^0)^\vee \leftarrow (\text{Cl}_l^0(K))^\vee \leftarrow 1.$$

We will show in corollary 8 that this sequence dual to the sequence 2 satisfies conditions of the theorem 5 and therefore  $\mathcal{C}_{K,l}^0$  is uniquely determined, since its dual  $(\mathcal{C}_{K,l}^0)^\vee$  is uniquely determined.

### 3 Proof of Lemmas

In this section we are going to prove all the necessarily lemmas needed for our proof. Let us start from recalling some basic facts about pro-finite abelian groups. A standard references are [5] and [4].

#### 3.1 Preliminaries

Let  $A$  an abelian, not necessarily topological group. If this group is finitely generated then the structure theorem says that  $A$  is isomorphic to  $\mathbb{Z}^r \oplus A_{\text{tors}}$  where  $r$  is a non-negative integer called rank and  $A_{\text{tors}}$  is a finite abelian group. Given two such groups we have that they are isomorphic if and only if they ranks and torsion parts coincide. The structure of an infinitely generated abelian group is more complicated. An element  $x$  of the abelian group  $A$  is *divisible* if for any  $n \in \mathbb{N}$  there exists  $y$  such that  $x = ny$ . A group  $A$  is *divisible* if all its elements are divisible. For example  $\mathbb{Q}$  is divisible. Another example is the so-called *Prüfer  $p$ -group* which is defined as union of all  $p^k$  roots of unity in  $\mathbb{C}^\times$  for a fixed prime number  $p$ :  $Z(p^\infty) = \{\zeta \in \mathbb{C}^\times \mid \zeta^{p^k} = 1, k \in \mathbb{N}\}$ . Note that we have



isomorphism of abstract groups:  $Z(p^\infty) \simeq \mathbb{Q}_p/\mathbb{Z}_p$ , where  $\mathbb{Q}_p$  denotes the abelian group of  $p$ -adic numbers and  $\mathbb{Z}_p$  is a subgroup of all  $p$ -adic integers.

A group is called *reduced* if it has no divisible elements.

**Lemma 3.** *Each abelian group  $A$  contains the maximal divisible subgroup  $D$  and is isomorphic to the direct sum of  $D$  and some reduced group  $R$ :  $A \simeq D \oplus R$ .*

*Proof.* Proof of this and the following lemma could be find at the chapter 3 of the book [4].  $\square$

The structure of the divisible subgroup is clear.

**Lemma 4.** *Any divisible group  $D$  is isomorphic to the direct sum of copies of  $\mathbb{Q}$  and  $Z(p^\infty)$ .*

The structure of the reduced part is more complicated and usually involves the theory of Ulms invariants. In this paper we will work with the reduced part directly not referring to the Ulms invariants at all.

### 3.1.1 The Pontryagin Duality

We need to recall some properties of the Pontryagin duality for locally compact abelian groups. A good reference including some historical discussion is [7]. Let  $\mathbb{T}$  be the topological group  $\mathbb{R}/\mathbb{Z}$  given with the quotient topology. If  $A$  is any locally compact abelian group one consider the Pontryagin dual  $A^\vee$  of  $A$  which is the group of all continuous homomorphism from  $A$  to  $\mathbb{T}$  :

$$A^\vee = \text{Hom}(A, \mathbb{T}).$$

This group has the so-called compact-open topology and is a topological group. Here we list some properties of the Pontryagin duality we use during the proof:

1. The Pontryagin duality is a contra-variant functor from the category of locally compact abelian groups to itself;
2. If  $A$  is a finite abelian group treated with the discrete topology then  $A^\vee \simeq A$  non-canonically;
3. We have the canonical isomorphism:  $(A^\vee)^\vee \simeq A$ ;
4. The Pontryagin dual to the pro-finite abelian group  $A$  is a discrete discrete torsion group and vice versa;

5. The Pontryagin duality sends direct products to direct sums and vice versa;
6. The Pontryagin dual of  $\mathbb{Z}_p$  is  $Z(p^\infty)$  and dual of  $\mathbb{Q}/\mathbb{Z}$  is the group of pro-finite integers  $\widehat{\mathbb{Z}}$ .

Having stated this we are able to prove our lemmas.

**Proof of Lemma 1.** Let  $A$  and  $B$  be two pro-finite abelian groups such that  $A \oplus \widehat{\mathbb{Z}} \simeq B \oplus \widehat{\mathbb{Z}}$ . Applying the Pontryagin duality to the above isomorphism we obtain:

$$(A)^\vee \oplus \mathbb{Q}/\mathbb{Z} \simeq (B)^\vee \oplus \mathbb{Q}/\mathbb{Z}.$$

Now since each abelian group is isomorphic to the direct sum of its reduced and divisible components and using the fact that  $\mathbb{Q}/\mathbb{Z}$  is divisible we have that reduced part of  $(A)^\vee$  and  $(B)^\vee$  are isomorphic. Now, according to the Lemma 4 each divisible part of  $(A)^\vee \oplus \mathbb{Q}/\mathbb{Z}$  is direct sum of copies of  $\mathbb{Q}$  and  $Z(p^\infty)$  and since  $\mathbb{Q}/\mathbb{Z} \simeq \bigoplus_p Z(p^\infty)$  divisible parts of  $(A)^\vee$  and  $(B)^\vee$  are isomorphic. Therefore  $(A)^\vee$  and  $(B)^\vee$  are isomorphic and hence  $A \simeq B$ .

□

### 3.2 Class Field Theory

We will start from the description of local aspects of the class field theory. Let  $L$  be a local field of positive characteristic  $p > 0$ . In other words  $L$  is a completion of a global function field  $K$  with respect to the discrete valuation associated to the place  $v$  of  $K$ . This field is isomorphic to the field of Laurant series with constant field  $\mathbb{F}_{q^n}$  and the corresponding ring of integers  $\mathcal{O}_L$  is the ring of formal power series:  $L \simeq \mathbb{F}_{q^n}((x))$ ,  $\mathcal{O}_L \simeq \mathbb{F}_{q^n}[[x]]$ . One way to construct abelian extensions of  $L$  is to take the algebraic closure  $\overline{\mathbb{F}_{q^n}}$  of the constant field  $\mathbb{F}_{q^n}$  which has Galois group  $\text{Gal}(\overline{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}) \simeq \widehat{\mathbb{Z}}$ . This is the maximal unramified abelian extension of  $L$ . Another way to construct abelian extensions is to add to  $L$  a root of the equation  $x^e - t = 0$ , where  $e$  is natural number such that  $\gcd(e, p) = 1$ . This is totally ramified extension. Denoting by  $I_L = \text{Gal}^{ram}(L^{ab} : L)$  the inertia subgroup of  $\mathcal{G}_L^{ab}$  we have the following split exact sequence:

$$1 \rightarrow I_L \rightarrow \mathcal{G}_L^{ab} \rightarrow \widehat{\mathbb{Z}} \rightarrow 1.$$

Recall that we also have the split exact sequence given via the valuation map:

$$1 \rightarrow \mathcal{O}_L^\times \rightarrow L^\times \rightarrow \mathbb{Z} \rightarrow 1.$$

The crucial point is that the local Artin map:  $L^\times \rightarrow \mathcal{G}_L^{ab}$  induces isomorphism of topological groups between the completion  $\widehat{L^\times}$  of  $L^\times$  and  $\mathcal{G}_L^{ab}$  such that two exact sequences are isomorphic:

$$\begin{array}{ccccccc} 1 \longrightarrow & \widehat{\mathcal{O}_L^\times} \simeq \mathcal{O}_L^\times & \longrightarrow & \widehat{L^\times} & \longrightarrow & \widehat{\mathbb{Z}} & \longrightarrow 1 \\ & \downarrow & & \downarrow & & \downarrow & \\ 1 \longrightarrow & I_L & \longrightarrow & \mathcal{G}_L^{ab} & \longrightarrow & \text{Gal}(\overline{\mathbb{F}_{q^n}} : \mathbb{F}_{q^n}) & \longrightarrow 1 \end{array}$$

Now if  $K$  is a global function field then it is possible to give a similar description of  $\mathcal{G}_K^{ab}$  via Idele-class group. Let  $\mathcal{I}_K$  denotes the multiplicative group of Ideles of  $K$ . This is the restricted direct product  $\mathcal{I}_K = \prod'_v K_v^\times$ , this product is taken over places  $v$  of  $K$  with respect to  $\mathcal{O}_v^\times$ . One defines the basic open sets as  $U = \prod'_v U_v$ , where  $U_v$  open in  $K_v^\times$  and almost all  $U_v = \mathcal{O}_v^\times$ . Under the topology generated by such  $U$  this becomes a topological group. The multiplicative group  $K^\times$  is embedded to  $\mathcal{I}_K$  diagonally as discrete subgroup and the quotient  $\mathcal{C}_K$  is the *Idele class group* of  $K$ . This is a topological group, but not pro-finite. One defines the global Artin map  $\mathcal{C}_K \rightarrow \mathcal{G}_K^{ab}$ . This map is injective, but not surjective. Similar to the local case it induces isomorphism of the pro-finite completion of  $\mathcal{C}_K$  and  $\mathcal{G}_K^{ab}$  as topological groups:  $\widehat{\mathcal{C}_K} \simeq \mathcal{G}_K^{ab}$ .

### 3.3 Deriving the main exact sequence

Now our goal is to derive the exact sequence 1. Let  $\mathcal{I}_K^0$  be the group of degree zero Ideles of  $K$ . It means the kernel of the degree map from  $\mathcal{C}_K$  to  $\mathbb{Z}$ . We have :

$$1 \rightarrow K^\times \rightarrow \mathcal{I}_K^0 \rightarrow \mathcal{C}_K^0 \rightarrow 1.$$

Let  $\mathcal{P}(K)$  denotes the group of ideals of  $K$  and  $\mathcal{P}^0(K)$  be the kernel of the degree map to  $\mathbb{Z}$ . We also have:

$$1 \rightarrow \mathbb{F}_q^\times \rightarrow K^\times \rightarrow \mathcal{P}^0(K) \rightarrow \text{Cl}^0(K) \rightarrow 1.$$

There is a surjective homomorphism  $\alpha$  of topological groups from  $\mathcal{I}_K^0$  to  $\mathcal{P}^0(K)$ , sending an Idele  $(a_{P_1}, a_{P_2}, \dots)$  to the divisor  $\sum v_{P_i}(a_{P_i}) \cdot P_i$ . This is well-defined since for a given Idele almost all  $a_P \in \mathcal{O}_{v_P}^\times$ . The kernel of this map is  $\prod_v \mathcal{O}_v^\times$ . Moreover, this map sends principal Ideles to principal ideals and hence induces the surjective quotient

map  $\hat{\alpha}$  from  $\mathcal{C}_K^0$  to  $\text{Cl}^0(K)$ . We have the following snake-lemma diagram:

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & \mathbb{F}_q^\times & \longrightarrow & \prod_v \mathcal{O}_v^\times & \longrightarrow & \ker \hat{\alpha} \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & K^\times & \longrightarrow & \mathcal{I}_K^0 & \longrightarrow & \mathcal{C}_K^0 \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & K^\times / \mathbb{F}_q^\times & \longrightarrow & \mathcal{P}^0(K) & \longrightarrow & \text{Cl}^0(K) \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & \longrightarrow & 1 & \longrightarrow & 1
 \end{array}$$

And therefore we have:

$$1 \rightarrow \mathbb{F}_q^\times \rightarrow \prod_v \mathcal{O}_v^\times \rightarrow \mathcal{C}_K^0 \rightarrow \text{Cl}^0(K) \rightarrow 1.$$

### 3.4 On the Structure of the Kernel

Now we will give an explicit description of the group  $\ker \hat{\alpha} \simeq (\prod_v \mathcal{O}_v^\times) / \mathbb{F}_q^\times$ . If  $v$  is a place of degree  $n$  a global function field  $K$  with the exact constant field  $\mathbb{F}_q$ , then  $K_v$  is the field of Laurant series with constant field  $\mathbb{F}_{q^n}$  and  $\mathcal{O}_v$  is the ring of formal power series:  $K_v \simeq \mathbb{F}_{q^n}((x))$ ,  $\mathcal{O}_v \simeq \mathbb{F}_{q^n}[[x]]$ . A formal power series is invertible if and only if it has non-zero constant term and therefore:

$$\mathcal{O}_v^\times \simeq \mathbb{F}_{q^n}^\times \times (1 + t\mathbb{F}_{q^n}[[t]]).$$

**Lemma 5.** *We have isomorphism of topological groups:  $1 + t\mathbb{F}_{q^n}[[t]] \simeq \prod_{\mathbb{N}} \mathbb{Z}_p$ .*

*Proof.* See [8], section on local fields. □

Denoting by  $\mathcal{T}_q$  the group  $(\prod_v \mathbb{F}_{q^{\deg(v)}}^\times) / \mathbb{F}_q^\times$ , we obtain:

$$(\prod_v \mathcal{O}_v^\times) / \mathbb{F}_q^\times \simeq \mathcal{T}_q \times \mathbb{Z}_p^\infty.$$

### 3.4.1 Description of $\mathcal{T}_q$

At the first time it seems that the group  $\mathcal{T}_q$  depends on  $K$  since the product  $\prod_v \mathcal{O}_v^\times$  is taken over all places of  $K$ . Our first goal is to show that it actually depends only on  $q$ . **Recall that:** because of the Weil-bound each function field  $K$  has places of all except finitely many degrees.

Consider the group  $A_q = \prod_v \mathbb{F}_{q^{\deg(v)}}^\times$ . By the Chinese reminder theorem we have:

$$A_q = \prod (\mathbb{Z}/l^m \mathbb{Z})^{a_{l,m}},$$

where  $a_{l,m}$  is either a non-negative integer or infinity. Since  $\mathbb{F}_{q^n}^\times$  is a cyclic group of order  $q^n - 1$  we have the direct description of  $a_{l,m}$ : it is the cardinality of the set  $\{v \in \text{Pl}(K) \mid \deg(v) = n, \text{ord}_l(q^n - 1) = m\}$ . Note that  $a_{p,m} = 0$  for all  $m \in \mathbb{N}$ .

**Lemma 6.** *Each  $a_{l,m}$  is either 0 or infinity.*

*Proof.* Indeed, suppose that there exists a place  $v$  of degree  $n$  such that  $\text{ord}_l(q^n - 1) = m$ , we would like to show that then there are infinitely many such  $v$ . Our assumption is equivalent to the statement that  $q^n \equiv 1 \pmod{l^m}$ , but  $q^n \not\equiv 1 \pmod{l^{m+1}}$ . The order of the group  $(\mathbb{Z}/l^{m+1} \mathbb{Z})^\times$  is  $\phi(l^{m+1}) = l^{m+1} - l^m$ , where  $\phi(a)$  denotes the Euler  $\phi$ -function. It means if  $q^n$  satisfies our condition then for any  $k \in \mathbb{N}$  the quantity  $q^{n+k\phi(l^{m+1})}$  also satisfies our condition. In other words, this condition depends only on  $n \pmod{\phi(l^{m+1})}$ . Since each function field  $K$  has places of all except finitely many degrees if there is one  $v$  then there are infinitely many.  $\square$

Now, given  $l \neq p$  we would like to understand how many  $m$  such that  $a_{l,m} = 0$  do we have. First we will prove the following elementary number theory lemma.

**Lemma 7.** *Let  $a$  be a positive integer such that  $\text{ord}_l(a - 1) = n$  for some prime number  $l$ . Then if  $l \neq 2$  or  $n \geq 2$  we have  $\text{ord}_l(a^l - 1) = n + 1$ .*

*Proof.* By the assumption of the lemma there exists an integer  $b$  such that  $\gcd(b, l) = 1$  and  $a = 1 + bl^n \pmod{l^{n+1}}$ . Suppose that  $l \neq 2$ . For some integer  $c$  we have:

$$\begin{aligned} a^l &= (1 + bl^n + cl^{n+1})^l = 1 + l(bl^n + cl^{n+1}) + \frac{l(l-1)}{2}(bl^n + cl^{n+1})^2 + \dots = \\ &= 1 + l^{n+1}(b + cl) + \frac{l(l-1)}{2}l^{2n}(b + cl)^2 + \dots \end{aligned}$$

Since  $l \neq 2$  we have  $a^l \equiv 1 + bl^{n+1} \pmod{l^{m+2}}$ .

Now let  $l = 2$  and  $n \geq 2$ . We have:  $a = 1 + 2^n + b2^{n+1} \pmod{2^{n+2}}$  and therefore  $a^2 \equiv 1 + 2^{n+1} \pmod{2^{n+2}}$ .  $\square$

**Lemma 8.** *For each odd prime number  $l$  different from  $p$  there exists  $N(l)$  such that  $a_{l,m}$  is infinite if and only if  $m \geq N(l)$ . Moreover  $N(l)$  depends only on  $q$  and doesn't depend on  $K$ .*

*Proof.* Let  $d = l - 1$  and  $N(l) = \text{ord}_l(q^d - 1)$ . Then  $q^d = 1$  in the group  $(\mathbb{Z}/l^{N(l)}\mathbb{Z})^\times$ , but  $q^d \neq 1$  in the group  $(\mathbb{Z}/l^{N(l)+1}\mathbb{Z})^\times$ . Therefore, for each  $u \in \mathbb{N}$  such that  $u \equiv d \pmod{\phi(l^{N(l)+1})}$  we have:  $\text{ord}_l(q^u - 1) = N(l)$ . Since  $K$  has places of almost all degrees the set  $\{v \in \text{Pl}(K) \mid \deg(v) \equiv d \pmod{\phi(l^{N(l)+1})}\}$  is infinite and hence  $a_{l,N(l)} \neq 0$ . We would like to show that if  $a_{l,m} \neq 0$  then  $a_{l,m+1} \neq 0$ . We know that there exists a place of the degree  $d_0$  such that  $\text{ord}_l(q^{d_0} - 1) = m$ . By the previous lemma we have  $\text{ord}_l(q^{ld_0} - 1) = m + 1$ . Then for any place  $v$  from the set  $\{v \in \text{Pl}(K) \mid \deg(v) \equiv ld_0 \pmod{\phi(l^{m+2})}\}$  we have  $\text{ord}_l(q^{\deg(v)} - 1) = m + 1$ . This shows that if  $m \geq N(l)$  then  $a_{l,m}$  is infinite.

The last step is to show that  $a_{l,m} = 0$  if  $m$  is less than  $\text{ord}_l(q^d - 1)$ . Indeed, the order  $a$  of  $q$  in the group  $\mathbb{F}_l^\times$  divides  $(l-1)$  and then  $\text{ord}_l(q^a - 1) = \text{ord}_l(q^{a \frac{l-1}{a}} - 1) = \text{ord}_l(q^{l-1} - 1)$ , since  $\frac{l-1}{a}$  is co-prime to  $l$ . It means that if for some  $u$  we have  $q^u \equiv 1 \pmod{l}$ , then  $u = ab$  and  $\text{ord}_l(q^u - 1) = \text{ord}_l(q^{ab} - 1) \geq \text{ord}_l(q^a - 1) = \text{ord}_l(q^{l-1} - 1)$ . □

**Lemma 9.** *For  $l = 2$  the following holds.*

1. *If  $p = 2$ , then  $a_{m,2} = 0$  for all  $m$ ;*
2. *if  $q \equiv 1 \pmod{4}$ , then there exists  $N(2)$  such that  $a_{2,m}$  is infinite if and only if  $m \geq N(2)$ ;*
3. *if  $q \equiv 3 \pmod{4}$ , then there exists  $N(2)$  such that  $a_{2,m}$  is infinite if and only if  $m \geq N(2)$  or  $m = 1$ ;*

*Proof.* The first statement is trivial. For the second one let  $N(2) = \text{ord}_2(q - 1)$ , then  $N(2) \geq 2$ . As before we have  $q \equiv 1 \pmod{2^{N(2)}}$ , but  $q \not\equiv 1 \pmod{2^{N(2)+1}}$ . The group  $(\mathbb{Z}/2^{N(2)+1}\mathbb{Z})^\times$  has order  $\phi(2^{N(2)+1})$  and hence, for each  $m$  such that  $m \equiv 1 \pmod{\phi(2^{N(2)+1})}$  we have that  $q^m \equiv 1 \pmod{2^{N(2)}}$ , but  $q \not\equiv 1 \pmod{2^{N(2)+1}}$ . Since  $K$  has places of almost all degrees the set  $\{v \in \text{Pl}(K) \mid \deg(v) \equiv 1 \pmod{\phi(2^{N(2)+1})}\}$  is infinite and hence  $a_{2,N(2)} \neq 0$ . Now, as in the previous lemma if  $a_{l,m} \neq 0$ , then  $a_{l,m+1}$  is not zero<sup>2</sup> and obviously if  $m < N(2)$  we have  $a_{2,m} = 0$ .

Finally suppose that  $q \equiv 3 \pmod{4}$ . By the same argument as before we have that  $a_{2,1}$  is infinite, but then  $q^2 \equiv 1 \pmod{8}$  and hence  $a_{2,2} = 0$ . Let  $N(2) = \text{ord}_2(q^2 - 1) \geq 3$ .

---

<sup>2</sup> here we use the fact that  $m \geq 2$ .

We have that for  $a_{2,N(2)}$  is infinite and for all  $k$  such that  $1 < k < N(2)$  we have  $a_{2,k} = 0$ . Because of the same argument as before  $a_{2,m}$  is infinite for all  $m \geq N(2)$ .  $\square$

In order to show that  $T_q \simeq A_q$  we need one elementary lemma.

**Lemma 10.** *For a given prime power  $q$  there are infinitely many integer numbers  $n$  such that  $\gcd(\frac{q^n-1}{q-1}, q-1) = 1$ .*

*Proof.* Consider the factorization of  $q-1$  into different prime factors:  $q-1 = l_1^{k_1} \dots l_m^{k_m}$ . We know that  $q \equiv 1 \pmod{l_i^{k_i}}$  and  $q \not\equiv 1 \pmod{l_i^{k_i+1}}$ , for all  $i$  in  $\{1, \dots, m\}$ . In other words there exists a natural number  $a_i$  co-prime to  $l_i$  such that  $q = 1 + a_i l_i^{k_i} \pmod{l_i^{k_i+1}}$ . Therefore if the natural number  $n$  is co-prime to  $q-1$  then  $q^n = 1 + a_i n l_i^{k_i} \pmod{l_i^{k_i+1}}$  and then  $\gcd(\frac{q^n-1}{q-1}, q-1) = 1$ .  $\square$

**Corollary 6.** *We have isomorphism  $A_q \simeq \mathcal{T}_q$ . The characteristic  $p$  of the constant field of  $K$  is determined by  $\mathcal{T}_q$ .*

*Proof.* For the first statement recall that  $\mathbb{F}_q^\times$  is embedded diagonally to the product  $\prod_v \mathbb{F}_{q^{\deg(v)}}^\times$ . Now pick any prime  $\beta$  of  $K$  of degree  $m$  such that  $\gcd(\frac{q^m-1}{q-1}, q-1) = 1$  and split the last product into two parts  $\mathbb{F}_{q^m}^\times \oplus \prod_{v \neq \beta} \mathbb{F}_{q^{\deg(v)}}^\times$ . Note that  $\mathbb{F}_q^\times$  is a subgroup of  $\mathbb{F}_{q^m}^\times$  which is direct summand. Since all these groups have the discrete topology, the quotient  $\prod_{v \neq \beta} \mathbb{F}_{q^{\deg(v)}}^\times \oplus (\mathbb{F}_{q^m}^\times / \mathbb{F}_q^\times)$  is topologically isomorphic to  $\mathcal{T}_q$ . Finally, since each  $a_{n,l}$  is either zero or infinity we have that  $A_q \simeq \mathcal{T}_q$ .

For the second statement note that  $p$  is unique prime such that  $a_{p,m} = 0$  for all  $m \in \mathbb{N}$ .  $\square$

**Lemma 11.** *For odd prime number  $l$  we have  $N(l) = \text{ord}_l(p^{l-1} - 1) + \text{ord}_l d_K$ .*

*Proof.* Recall the isomorphism  $\mathbb{Z}_l^\times \simeq (\mathbb{Z}_l)_{\text{tors}}^\times \times (1 + l\mathbb{Z}_l)$ , for  $l$  be an odd prime number. The multiplicative group  $1 + l\mathbb{Z}_l$  has the following filtration:

$$1 \subset 1 + l\mathbb{Z}_l \subset 1 + l^2\mathbb{Z}_l \subset \dots$$

Given  $q$  and  $l \neq p$  let  $d$  be the order of  $q \in (\mathbb{Z}_l)_{\text{tors}}^\times$ . Then by our construction  $N(l)$  is the greatest integer such that  $q^d \in 1 + l^{N(l)}\mathbb{Z}_l$ . Raising  $q$  to the power  $p$  doesn't change the filtration. On the other hand, lemma 7 shows that raising  $q$  to the power  $l$  shifts the filtration exactly at one. Hence for  $q = p^{d_K p^n}$ ,  $\gcd(d_K, p) = 1$  we have:

$$N(l) = \text{ord}_l(q^{l-1} - 1) = \text{ord}_l(p^{(l-1)d_K p^k} - 1) = \text{ord}_l(p^{l-1} - 1) + \text{ord}_l(d_K)$$

$\square$

Recall that for a prime number  $l$  different from  $p$  we define  $s_l(\mathcal{T}_q)$  to be the least integer  $k$  such that  $T_q$  has direct summand of the form  $\mathbb{Z}/l^k\mathbb{Z}$ . Obviously, if  $l \neq 2$  then  $s_l(T_q) = N(l)$ . More generally, we have:

**Lemma 12.** *The natural number  $d_K$  is a unique number such that for any prime number  $l \neq p$ :*

$$\text{ord}_l(d_K) = \begin{cases} 0, & \text{if } l = 2 \text{ and } s_2 = 1 \\ s_l(\mathcal{T}_q) - \text{ord}_l((p^*)^{l-1} - 1), & \text{otherwise.} \end{cases}$$

*Proof.* The case of the odd  $l$  is clear, since  $p^* = (-1)^{\frac{p-1}{2}}p$  if  $p$  is odd and hence for  $l = 1 \pmod 2$  we have  $(p^*)^{l-1} = p^{l-1}$ . If  $l = 2$  then there are two cases. If  $p = 1 \pmod 4$  then  $s_2(T_q) = N(2)$  and obviously  $p^* = p$ , hence our formula holds trivially. If  $p = 3 \pmod 4$  then either  $q = 3 \pmod 4$  or  $q = 1 \pmod 4$ . In the first case we have  $d_K = 1 \pmod 2$  and  $s_2(\mathcal{T}_q) = 1$  which leads to the our "exceptional case". In the second case we have  $d_K = 0 \pmod 2$  and then  $N(2) = s_2(T_q) \geq 2$  and hence  $s_2(T_q) = \text{ord}_2(q-1) = \text{ord}_2(p^{p^*d_K} - 1) = \text{ord}_2(p^{2\frac{d_K}{2}} - 1) = \text{ord}_2(p^2 - 1) + \text{ord}_2(d_K) - 1 = \text{ord}_2(p+1) + \text{ord}_2(d_K) = \text{ord}_2(p^* - 1) + \text{ord}_2(d_K)$ , since in this case  $p^* = -p$ .  $\square$

Now we are able to prove our main result concerning isomorphism type of the abelian group  $\mathcal{T}_q$ . For a prime power  $q = p^n$  we define  $d_q$  to be the non- $p$  part of  $n$  :  $d_q = \frac{n}{p^{\text{ord}_p n}}$ . Trivially, for a function field  $K$  with the exact constant field  $\mathbb{F}_q$  we have  $d_K = d_q$ .

**Theorem 6.** *Given two powers of  $p$ :  $q_1 = p^{n_1}$  and  $q_2 = p^{n_2}$  groups  $\mathcal{T}_{q_1}$  and  $\mathcal{T}_{q_2}$  are isomorphic if and only if  $d_{q_1} = d_{q_2}$ .*

*Proof.* The only invariants of  $T_q$  are the sequence of coefficients  $a_{l,m}$  for different  $l, m$ . We will show that they coincide for all  $l, m$  if and only if the condition of the our theorem holds.

First we will prove the if part. We know that  $d_{q_1} = d_{q_2}$ . Let  $l$  be an odd prime number different from  $p$ , then by the formula from the above lemma  $s_l(\mathcal{T}_{q_1}) = s_l(\mathcal{T}_{q_2})$  and we have  $a_{l,m} = 0$  if and only if  $m < s_l(\mathcal{T}_{q_1})$  which shows that coefficients  $a_{m,l}$  coincide for  $\mathcal{T}_{q_1}$  and  $\mathcal{T}_{q_2}$ . Suppose that  $l = 2$ . If  $p = 2$  then  $a_{2,m} = 0$  for all  $m$  in both groups. If  $p = 1 \pmod 4$  or  $d_{q_1} = 0 \pmod 2$  then as before  $a_{2,m} = 0$  if and only if  $m < N_2(l) = s_2(T_{q_1}) = \text{ord}_2(d_{q_1}) + \text{ord}_2(p-1)$  and hence  $a_{2,m}$  coincide for both groups. Finally, if  $p = 3 \pmod 4$  and  $d_{q_1} = d_{q_2} = 1 \pmod 2$  then  $a_{2,m} = 0$  if and only if either  $m = 1$  or  $m > N(2) = \text{ord}_2(q_1^2 - 1) = \text{ord}_2(q_2^2 - 1)$ . The equality  $\text{ord}_2(q_1^2 - 1) = \text{ord}_2(q_2^2 - 1)$  holds since:  $\text{ord}_2(q_1^2 - 1) = \text{ord}_2(q_1 + 1) + 1 = \text{ord}_2(p^{d_{q_1}p^k} + 1) + 1 = \text{ord}_2(p + 1) + 1$ .

Now, suppose that  $T_{q_1} \simeq T_{q_2}$ . Then by the formula from lemma 12 for any odd prime number  $l$  different from  $p$  we have  $\text{ord}_l(d_{q_1}) = \text{ord}_l(d_{q_2})$ . By definition we have



$\text{ord}_p(d_{q_1}) = \text{ord}_p(d_{q_2}) = 0$ . Finally, for  $l = 2$  there are two cases. Either both groups contain direct summand of the form  $\mathbb{Z}/2\mathbb{Z}$  and then  $\text{ord}_2(d_{q_1}) = \text{ord}_2(d_{q_2}) = 0$ , or otherwise the formula from lemma 12 holds and then  $\text{ord}_2(d_{q_1}) = \text{ord}_2(d_{q_2})$ .  $\square$

This already gives some important corollary. Let  $q = 2^{2^k}$  for some non-negative integer  $k$ , then coefficients  $a_{l,m}$  defined as follows:

$$a_{l,m} = \begin{cases} \mathbb{N}, & \text{if } l \neq 2 \text{ and } m \geq \text{ord}_l(2^{l-1} - 1) \\ 0, & \text{otherwise.} \end{cases}$$

**Corollary 7.** *The following function fields of characteristic two share the same abelianized absolute Galois group  $\mathcal{G}_K^{ab} \simeq \prod_{l,m} (\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}} \times \prod_{\mathbb{N}} \mathbb{Z}_2 \oplus \widehat{\mathbb{Z}}$  :*

1. *The rational function field with  $g = 0$  over  $\mathbb{F}_{2^{2^k}}$ , for any non-zero integer  $k$ ;*
2. *The elliptic function field  $y^2 + y = x^3 + x + 1$ , with  $g = 1$  over  $\mathbb{F}_2$ ;*
3. *The hyper elliptic function field  $y^2 + y = x^5 + x^3 + 1$ , with  $g = 2$  over  $\mathbb{F}_2$ ;*
4. *The hyper elliptic function field  $y^2 + y = (x^3 + x^2 + 1)(x^3 + x + 1)^{-1}$ , with  $g = 2$  over  $\mathbb{F}_2$ ;*
5. *The function field of the plane quartic  $y^4 + (x^3 + x + 1)y + (x^4 + x + 1) = 0$ , with  $g = 3$  over  $\mathbb{F}_2$ .*
6. *The elliptic function field  $y^2 + y = x^3 + \mu$ , with  $g = 1$  over  $\mathbb{F}_4$ , where  $\mu$  is the generator of  $\mathbb{F}_4^\times$ .*

*In particular, the genus, the constant field and the zeta-function of  $K$  are not determined by  $G_K^{ab}$ .*

*Proof.* All these fields have trivial  $\text{Cl}^0(K)$ , see [6]. Since  $\mathcal{T}_2 \simeq \mathcal{T}_{2^{2^k}}$  we have that for any  $K$  listed above  $\mathcal{C}_K^0 \simeq \mathcal{T}_2 \times \prod_{\mathbb{N}} \mathbb{Z}_2$ .  $\square$

**Remark:** For given  $q$  we will call a prime  $l$  *exceptional* if  $N(l) > 1$ . The question which  $l$  are exceptional seems to be very difficult. Of course, if  $l^2 | (q - 1)$ , then  $a_{l,1} = 0$ . For example if  $q = 9$  then  $a_{2,1} = a_{2,2} = 0$ . But also there are exceptional primes  $l$  with  $\gcd(l, q - 1) = 1$ . For example if  $p = q = 7$  and  $l = 5$ . Then if  $7^d = 1 \pmod{5}$  if and only if  $d = 4k$ , but then  $7^d = 49^{2k} = (-1)^{2k} = 1 \pmod{25}$ . It means that 5 is exceptional. We expect that for a given  $q$  there are infinitely many exceptional primes, but we have no idea how to prove it even for the case  $q = 2$ : the first exceptional prime for this case is 1093. This phenomena is strictly related with the so-called *Wieferich primes*.

### 3.5 On the torsion of $\mathcal{C}_K^0$

Now our goal is to understand what happens with the exact sequence  $1 \rightarrow \mathcal{T}_q \times \mathbb{Z}_p^\infty \rightarrow \mathcal{C}_K^0 \rightarrow \text{Cl}^0(K) \rightarrow 1$ , when  $\text{Cl}^0(K)$  is not trivial. Since we are working with infinite groups  $\mathcal{C}_K^0$  could still be isomorphic to the group mentioned in the corollary 7.

**Theorem 7.** *All the torsion of  $\mathcal{C}_K^0$  are in  $\mathcal{T}_q$ , hence the exact sequence 1 is totally non-split. Moreover, the topological closure of the torsion subgroup of  $\mathcal{C}_K^0$  is  $\mathcal{T}_q : \overline{\mathcal{C}_K^0[\text{tors}]} = \mathcal{T}_q$ .*

*Proof.* Suppose that there exists a non-zero  $x \in \mathcal{C}_K^0$  such that  $x^l = 0$  for some prime number  $l$ , not necessarily co-prime to  $p$ . We would like to show that actually this element has trivial image in the class group. Pick a representative  $(x_1, x_2, \dots)$  for  $x$  as element of  $\mathcal{I}_K$ , we know that almost all  $x_i \in \mathcal{O}_v^\times$  and that  $x^l = (x_1^l, x_2^l, \dots)$  is a principal Idele. Let  $a$  be the element of  $K^\times$  whose image in  $\mathcal{I}_K$  is  $x^l$ . We have that  $a$  is locally an  $l$ -th power and hence by [theorem 1, chapter 9] from [2] we have that  $a$  is globally an  $l$ -th power and hence  $x$  is a principal Idele up to multiplication by the element  $(\zeta_1, \zeta_2, \dots) \in \mathcal{T}_q$ , where  $\zeta_i$  denotes an  $l$ -th root of unity and hence its image in the class group is trivial.

Since  $\mathbb{Z}_p$  is torsion free we have that all the torsion of  $\mathcal{C}_K^0$  lies in  $\mathcal{T}_q$ . Note that each element of finite order in  $\mathcal{T}_q$  is an element of the direct sum  $\bigoplus_{l,m} (\mathbb{Z}/l^m\mathbb{Z})^{a_{l,m}}$  and closure of this direct sum is  $\mathcal{T}_q$  itself.  $\square$

As it was mentioned in the introduction this statement implies the "only if" part of our main result.

### 3.6 Proof of the inverse implication

Our task in this section is for given  $K$  show that the data  $\text{Cl}_{non-p}^0(K), \mathcal{T}_q$  determines  $\mathcal{C}_K^0$  up to isomorphism.

#### 3.6.1 The $p$ -part

Our first goal is to show that the  $p$ -part of  $\mathcal{C}_K^0$  is isomorphic to  $\mathbb{Z}_p^\infty$ .

We start from an easy example. Consider the exact sequence:  $0 \rightarrow \mathbb{Z}_p \rightarrow \mathbb{Z}_p \rightarrow \mathbb{Z}/p^k\mathbb{Z} \rightarrow 0$ , where the second map is multiplication by  $p^k$ . This sequence is totally non-split. We claim that  $\mathbb{Z}_p$  is a unique group which could occur in the middle of this sequence. More concretely:

**Example 1.** *Let  $A$  be an abelian pro- $p$  group such that the following sequence is totally non-split:  $0 \rightarrow \mathbb{Z}_p \rightarrow A \rightarrow \mathbb{Z}/p^k\mathbb{Z} \rightarrow 0$ , then  $A \simeq \mathbb{Z}_p$ .*

*Proof.* Since  $\mathbb{Z}_p$  is torsion free and the sequence is totally non-split then  $A$  is also torsion free. Let us denote the quotient map by  $\phi$ . There exists  $x \in A$  such that  $\phi(x)$  is the generator of  $\mathbb{Z}/p^k\mathbb{Z}$ . Moreover, since  $A$  is torsion free we know that  $p^k x$  is a non-zero element  $a = \phi(x)$  of  $\mathbb{Z}_p$ . We claim that the first non-zero coefficient in the  $p$ -adic expression  $a = a_0 + a_1p + a_2p^2 + \dots$  is  $a_0$ . Indeed, if  $a$  is divisible by  $p$  then  $p(x - a/p) = 0$  and hence  $x = a/2$  since  $A$  is torsion free. Then  $A$  is generated by  $\{x, \mathbb{Z}_p\}$  with the relation  $p^k x = a$ . Consider the map  $\psi : A \rightarrow \mathbb{Z}_p$ , which sends element  $x$  to  $a$  and  $\mathbb{Z}_p \rightarrow p^k \mathbb{Z}_p$ . Then  $\psi$  is homomorphism:  $\psi(p^k x) = \psi(a) = p^k a = p^k \psi(x)$ . The kernel of this map is trivial and since  $a_0 \neq 0$  then this map is onto.  $\square$

This example gives an idea how to prove the following:

**Lemma 13.** *Let  $A$  be an abelian pro- $p$  group such that the following sequence is totally non-split:  $0 \rightarrow \mathbb{Z}_p^\infty \rightarrow A \rightarrow B \rightarrow 0$ , where  $B$  is a finite abelian  $p$ -group. Then  $A \simeq \mathbb{Z}_p^\infty$ .*

*Proof.* Since the sequence is totally non-split and  $\mathbb{Z}_p$  is torsion free, then  $A$  is torsion free also. This means that multiplication by any natural number is injective. It means that the Pontryagin dual  $A^\vee$  of  $A$  is torsion (since  $A$  is pro-finite) and divisible (since the dual to the injection is surjection). Consider the dual sequence:  $0 \rightarrow B^\vee \rightarrow A^\vee \rightarrow \oplus \mathbb{Z}(p^\infty) \rightarrow 0$ . By the structure theorem of divisible groups  $A^\vee$  is isomorphic to the direct sum of copies of  $\mathbb{Z}(p^\infty)$  and  $\mathbb{Q}$ . But  $A^\vee$  is torsion and hence  $A \simeq \mathbb{Z}_p^\infty$ .  $\square$

This shows that  $\mathcal{C}_{K,p}^0$  depends only on  $p$  and since isomorphic  $T_q$  share the same  $p$  we conclude that  $\mathcal{C}_{K,p}^0$  is determined by the our data.

### 3.6.2 The non $p$ -part

Now we pick the prime number  $l \neq p$  and consider the  $l$ -part  $\mathcal{C}_{K,l}^0$  of  $\mathcal{C}_K^0$ . If  $l$  is such that  $\text{Cl}_l^0(K) \simeq \{0\}$  then obviously  $\mathcal{T}_{q,l} \simeq \mathcal{C}_{K,l}^0$ . Let  $l$  be a prime such that  $\text{Cl}_l^0(K)$  is not trivial. We know that the following sequence is totally non-split:

$$1 \rightarrow \mathcal{T}_{q,l} \rightarrow \mathcal{C}_{K,l}^0 \rightarrow \text{Cl}_l^0(K) \rightarrow 1.$$

Fix a natural number  $n$ . Then multiplication by  $l^n$  map induces the following commutative diagram:

$$\begin{array}{ccccccc}
1 & \longrightarrow & \mathcal{T}_{q,l}[l^n] & \hookrightarrow & \mathcal{C}_{K,l}^0[l^n] & \xrightarrow{0} & \text{Cl}_l^0(K)[l^n] \\
& & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & \mathcal{T}_{q,l} & \longrightarrow & \mathcal{C}_{K,l}^0 & \longrightarrow & \text{Cl}_l^0(K) \longrightarrow 1 \\
& & \downarrow l^n & & \downarrow l^n & & \downarrow l^n \\
1 & \longrightarrow & \mathcal{T}_{q,l} & \longrightarrow & \mathcal{C}_{K,l}^0 & \longrightarrow & \text{Cl}_l^0(K) \longrightarrow 1 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & \mathcal{T}_{q,l}/l^n \mathcal{T}_{q,l} & \longrightarrow & \mathcal{C}_{K,l}^0/l^n \mathcal{C}_{K,l}^0 & \longrightarrow & \text{Cl}_l^0(K)/l^n \text{Cl}_l^0(K) \longrightarrow 1
\end{array}$$

Since our main sequence is totally non-split the map from  $\mathcal{C}_{K,l}^0[l^n]$  to  $\text{Cl}_l^0(K)[l^n]$  is the zero map and the map from  $\mathcal{T}_{q,l}[l^n]$  to  $\mathcal{C}_{K,l}^0[l^n]$  is isomorphism. Now applying the Pontryagin duality to the above diagram we get:

$$\begin{array}{ccccccc}
1 & \longleftarrow & (\mathcal{T}_{q,l}[l^n])^\vee & \longleftarrow & (\mathcal{C}_{K,l}^0[l^n])^\vee & \xleftarrow{0} & (\text{Cl}_l^0(K)[l^n])^\vee \\
& & \uparrow & & \uparrow & & \uparrow \\
1 & \longleftarrow & (\mathcal{T}_{q,l})^\vee & \longleftarrow & (\mathcal{C}_{K,l}^0)^\vee & \longleftarrow & (\text{Cl}_l^0(K))^\vee \longleftarrow 1 \\
& & \uparrow l^n & & \uparrow l^n & & \uparrow l^n \\
1 & \longleftarrow & (\mathcal{T}_{q,l})^\vee & \longleftarrow & (\mathcal{C}_{K,l}^0)^\vee & \longleftarrow & (\text{Cl}_l^0(K))^\vee \longleftarrow 1 \\
& & \uparrow & & \uparrow & & \uparrow \\
& & (\mathcal{T}_{q,l}/l^n \mathcal{T}_{q,l})^\vee & \longleftarrow & (\mathcal{C}_{K,l}^0/l^n \mathcal{C}_{K,l}^0)^\vee & \longleftarrow & (\text{Cl}_l^0(K)/l^n \text{Cl}_l^0(K))^\vee \longleftarrow 1
\end{array}$$

Because of the construction of  $\mathcal{T}_{q,l}$  the group  $(\mathcal{T}_{q,l})^\vee$  is isomorphic to the direct sum of cyclic groups  $(\mathcal{T}_{q,l})^\vee \simeq \oplus_{k \geq N(l)} \oplus_{\mathbb{N}} \mathbb{Z}/l^k \mathbb{Z}$  and therefore  $\cap_n l^n (\mathcal{T}_{q,l})^\vee = \{0\}$ . It means we have  $(\cap_n l^n (\mathcal{C}_{K,l}^0)^\vee) \subset (\text{Cl}_l^0(K))^\vee$ . Our goal is to show that  $(\cap_n l^n (\mathcal{C}_{K,l}^0)^\vee) = (\text{Cl}_l^0(K))^\vee$ .

**Lemma 14.** *Given any non-zero element  $x$  of  $(\text{Cl}_l^0(K))^\vee \subset (\mathcal{C}_{K,l}^0)^\vee$  and any natural number  $n$  there exists element  $c_x \in (\mathcal{C}_{K,l}^0)^\vee$  such that  $l^n c_x = x$ .*

*Proof.* For fixed  $n$  consider the above diagram. Since the second row is exact the image of  $x$  in  $(\mathcal{T}_{q,l})^\vee$  is zero. Then its image in  $(\mathcal{T}_{q,l}[l^n])^\vee$  is also zero. Since  $(\mathcal{T}_{q,l}[l^n])^\vee \simeq (\mathcal{C}_{K,l}^0[l^n])^\vee$  it means that image of the non-zero element  $x$  in  $(\mathcal{C}_{K,l}^0[l^n])^\vee$  is zero. Since the second

column is exact this means that  $x$  lies in the image of the multiplication by  $l^n$  map from  $(\mathcal{C}_{K,l}^0)^\vee$  to  $(\mathcal{C}_{K,l}^0)^\vee$  and therefore there exists  $c_x$  such that  $l^n c_x = x$ .  $\square$

It means that we have proved:

**Corollary 8.** *The exact sequence  $1 \leftarrow (\mathcal{T}_{q,l})^\vee \leftarrow (\mathcal{C}_{K,l}^0)^\vee \leftarrow (\text{Cl}_l^0(K))^\vee \leftarrow 1$  satisfies conditions of the theorem 5.*

In order to finish our proof we need to prove theorem 5.

### 3.6.3 Proof of the Theorem 5

First, let us recall the settings.

**Theorem 8.** *Let  $\{C_i\}$  be a countable set of finite cyclic abelian  $l$ -groups with orders of  $C_i$  are not bounded as  $i$  tends to infinity and let  $A$  be any finite abelian  $l$ -group. Then up to isomorphism there exists and unique torsion abelian  $l$ -group  $B$  satisfying two following conditions:*

1. *There exists an exact sequence:  $1 \rightarrow A \rightarrow B \rightarrow \bigoplus_{i \geq 1} C_i \rightarrow 1$ ;*
2.  *$A$  is the union of all divisible elements of  $B$ :  $A = \bigcap_{n \geq 1} nB$ .*

**Proof of the existence.** Given a group  $A$  and  $\bigoplus_{i \geq 1} C_i$  let  $k_i$  denotes the order of the group  $C_i$ . Because of the assumptions of the theorem, the sequence of orders  $k_i$  is not bounded and hence for each natural number  $N$  there exists  $i$  such that  $k_i \geq N$ . Let us pick a sequence of indexes  $j_i$ ,  $i \in \mathbb{N}$  such that  $k_{j_i} \geq l^i$ . Let  $\alpha_0, \dots, \alpha_{n-1}$  be any finite set of generators of  $A$ . Consider the sequence  $a_m$  of elements of  $A$  defined as follows:

$$a_m = \begin{cases} \alpha_i \bmod n, & \text{if } m = j_i \\ 0, & \text{otherwise.} \end{cases}$$

Consider the abelian group  $B$  isomorphic to the quotient of the direct sum  $A \oplus (\bigoplus_{i \in \mathbb{N}} X_i \mathbb{Z})$  of countably many copies of  $\mathbb{Z}$  and one copy of  $A$  by the relations  $k_i X_i = a_i$ . We have that  $B$  contains  $A$  as a subgroup and the quotient of  $B$  by  $A$  is isomorphic to  $\bigoplus_i C_i$ . It means that the group  $B$  satisfies the first condition of the theorem. Now, consider the group  $Z = \bigcap_{n \geq 1} nB$ . Obviously,  $Z \subset A$  and we would like to show that actually  $Z = A$ . This follows from the fact that for any fixed number  $N > 1$  the set  $\{k_{j_i} X_{j_i} | i \geq \log_l N\}$  generates  $A$  and satisfies  $k_{j_i} \geq l^i \geq l^{\log_l(N)} \geq N$ .

**Proof of the uniqueness.** Suppose we are given an abelian torsion  $l$ -group  $B$  which satisfies both conditions of the our theorem. Denote the map from  $B$  to  $\bigoplus_{i \geq 1} C_i$  by  $\phi$ . Let  $\tilde{x}_i$  denotes a generator of the cyclic group  $C_i$  and let  $k_i$  denotes the order of  $C_i$ . Let  $x_i$  be an element of  $B$  such that  $\phi(x_i) = \tilde{x}_i$ , then  $k_i x_i \in A$ .

**Lemma 15.** *For any positive integer  $M$  which is a power of  $l$  the set  $A_M = \{k_i x_i | k_i \geq M\}$  generates  $A$ .*

*Proof.* Without loss of generality we assume that  $M \geq \#A$ . Pick a non-zero element  $a \in A$ . Because of the second property  $a$  could be written as  $M^2 y$ , where  $y \in B$ . Since the sequence  $1 \rightarrow A \rightarrow B \rightarrow \oplus_{i \geq 1} C_i \rightarrow 1$  is exact we could write  $y$  as finite combination of  $x_{i_j}$  and elements of  $A$ :  $y = b_{i_1} x_{i_1} + b_{i_2} x_{i_2} + \dots + b_{i_n} x_{i_n} + a_0$ . Pick the subset  $S$  of  $i_1, \dots, i_n$  consisting of indexes of  $i_j$  such that  $k_{i_j} \geq M$ . Since  $M^2 x_{i_j} = 0$  if  $k_{i_j} < M$  we have :  $M^2 \sum_{j \in S} b_{i_j} x_{i_j} = a$ . On the other hand  $0 = \phi(a) = M^2 \sum_{j \in S} b_{i_j} \tilde{x}_{i_j}$  and hence  $M^2 b_{i_j}$  is divisible by  $k_{i_j}$  and  $a = \sum_{j \in S} \frac{b_{i_j} M^2}{k_{i_j}} k_{i_j} x_{i_j}$ . Which means that  $\{k_i x_i | k_i \geq M\}$  generates  $A$ .  $\square$

**Remark:** consider the sequence  $a_i = k_i x_i$  of elements of  $A$  from the above lemma. We will say that this sequence  $\langle a_i \rangle$  *strongly generates*  $A$ .

Note that  $B$  as abstract abelian group is isomorphic to the group generated by elements  $X_i$  and  $a_i$  such that  $k_i X_i = a_i$ :  $B = \langle X_i, a_i \rangle / (k_i X_i - a_i)$ . Given another abelian group  $B'$  satisfying conditions of our theorem we know that  $B' = \langle X'_i, a'_i \rangle / (k_i X'_i - a'_i)$ . If for any  $i$  we have  $a_i = a'_i$  as elements of  $A$  then, obviously  $B \simeq B'$ . Our goal is to show that  $B \simeq B'$  in any case.

**Definition 2.** *Given two such groups  $B, B'$  consider the set  $S = \{i | a_i = a'_i\}$ . We will say that  $B$  and  $B'$  have large overlap if the set  $\{a_i | i \in S\}$  strongly generates  $A$ , i.e. that for any integer  $M$  the set  $S_M = \{a_i | i \in S, k_i \geq M\}$  generates  $A$ .*

We have the following observation:

**Lemma 16.** *If  $B$  and  $B'$  have large overlap, then they are isomorphic.*

*Proof.* For each index  $i$  consider the difference  $a_i - a'_i$ . Since  $B$  and  $B'$  have large overlap, we could write this difference as finite sum  $\sum_{m \in S} \lambda_m k_m X'_m$  with  $k_m \geq k_i$ . Since both  $k_m$  and  $k_i$  are powers of  $l$  the ratio  $\frac{k_m}{k_i}$  is an integer. Consider the map  $\psi$  from  $B$  to  $B'$  defined as follows. The map  $\psi$  is identity on  $A$ . If  $i \in S$  then  $\psi(X_i) = X'_i$ , otherwise  $\psi(X_i) = X'_i + \sum_{m \in S} \lambda_m \frac{k_m}{k_i} X'_m$ . We claim that  $\psi$  is a homomorphism: if  $i \in S$  then  $a_i = \psi(k_i X_i) = k_i \psi(X_i) = k_i X'_i = a'_i$ . If  $i \notin S$ , we have  $a_i = \psi(k_i X_i) = k_i (X'_i + \sum_{m \in S} \lambda_m \frac{k_m}{k_i} X'_m) = k_i X'_i + \sum_{m \in S} \lambda_m k_m X'_m = a'_i + (a_i - a'_i) = a_i$ . In other words it sends generators of  $B$  to elements of  $B'$  preserving all relations. We claim moreover that the map  $\psi$  is an isomorphism since we will construct the inverse map  $\phi$  from  $B'$  to  $B$  as follows. The map  $\phi$  is identity on  $A$ . For  $i \in S$  we have  $\phi(X'_i) = X_i$  and for  $i \notin S$

we have  $\phi(X'_i) = X_i - \sum_{m \in S} \lambda_m \frac{k_m}{k_i} X_m$ . Then, for  $i \notin S$  we have:

$$\begin{aligned} \phi(\psi(X_i)) &= \phi(X'_i + \sum_{m \in S} \lambda_m \frac{k_m}{k_i} X'_m) = \phi(X'_i) + \phi(\sum_{m \in S} \lambda_m \frac{k_m}{k_i} X'_m) = \\ &= (X_i - \sum_{m \in S} \lambda_m \frac{k_m}{k_i} X_m) + (\sum_{m \in S} \lambda_m \frac{k_m}{k_i} X_m) = X_i. \end{aligned}$$

□

Now we will prove:

**Corollary 9.** *Two groups  $B$  and  $B'$  satisfying conditions of the above theorem are isomorphic.*

*Proof.* Suppose that there exists a partition of the set of positive integers  $\mathbb{N}$  on two sets  $\mathbb{N} = I_1 \cup I_2$ ,  $I_1 \cap I_2 = \emptyset$  such that each of the set  $\{a_i | i \in I_1\}$  and  $\{a'_i | i \in I_2\}$  strongly generates  $A$ . Then we define abelian group  $D$  to be the quotient of the direct sum  $A \oplus (\oplus_{i \in \mathbb{N}} X_i \mathbb{Z})$  of countably many copies of  $\mathbb{Z}$  and one copy of  $A$  by the relations  $k_i X_i = a_i$ ,  $i \in I_1$  and  $k_i X_i = a'_i$ ,  $i \in I_2$ . Obviously  $D$  also satisfies conditions of the above theorem. Moreover  $D$  and  $B$  and also  $D$  and  $B'$  have large overlap, therefore  $B \simeq D \simeq B'$ .

Now we will show that such partition exists. We will construct this partition inductively. Let  $N_0 = 0$  and let  $N_1$  be the minimal integer such that elements of the set  $S_1 = \{a_i | i \leq N_1 \text{ and } k_i \geq l\}$  generate  $A$ . The reason for this number to exist is the following. The sequence  $a_i$  strongly generates  $A$  which implies that there exist indexes  $i$  with  $k_i \geq l$  such that  $a_i$  generate  $A$ , but  $A$  is a finite group and hence we could pick a finite number of elements with  $k_i \geq l$  generating  $A$ . Note that dropping out finitely many indexes doesn't affect the fact that each of the sequences  $a_i$  and  $a'_i$  strongly generates  $A$ . Suppose we've constructed the number  $N_m$  then let  $N_{m+1}$  be a minimal integer such that elements of the set

$$S_{m+1} = \begin{cases} \{a'_i | N_m < i \leq N_{m+1} \text{ and } k_i \geq l^{m+1}\}, & \text{if } m \text{ is odd} \\ \{a_i | N_m < i \leq N_{m+1} \text{ and } k_i \geq l^{m+1}\}, & \text{otherwise.} \end{cases}$$

generate  $A$ . Finally, we define  $I_1 = \cup_{m \geq 0} \{i \in \mathbb{N} | N_{2m} < i \leq N_{2m+1}\}$  and  $I_2 = \cup_{m \geq 1} \{i \in \mathbb{N} | N_{2m-1} < i \leq N_{2m}\}$ . □

## 4 Proof of Corollaries

In this section we will prove corollaries 1, 2 and 3. The first two will follow from the existence for a given constant field  $k = \mathbb{F}_q$  an elliptic curve  $E$  over  $k$  with the group  $E(\mathbb{F}_q)$  of  $\mathbb{F}_q$ -rational points having order  $q$ , since in the case of elliptic curves we have  $E(\mathbb{F}_q) \simeq \text{Cl}^0(K_E)$ , where  $K_E$  denotes the associated to  $E$  global function field.

**Definition 3.** *Fix a finite field  $\mathbb{F}_q$ . Let  $N$  be an integer number in the Hasse interval:  $N \in [-2\sqrt{q}; 2\sqrt{q}]$ . We will call it admissible if there exists an elliptic curve  $E$  over  $\mathbb{F}_q$  with  $q + 1 - \#E(\mathbb{F}_q) = N$ .*

The following statement is a part of the classical statement due to Waterhouse, for reference see [10]:

**Theorem 9** (Waterhouse). *If  $\gcd(p, N) = 1$  then the number  $N$  is admissible.*

**Corollary 10.** *Given a finite field  $\mathbb{F}_q$  there exists an elliptic curve  $E$  over  $\mathbb{F}_q$  with  $\#E(\mathbb{F}_q) = q$ .*

The above remarks finish the proof of corollaries 1 and 2. Now we will discuss the proof of the corollary 3. Our goal is to show :

**Theorem 10.** *Given a constant field  $k = \mathbb{F}_q$  with characteristic  $p \neq 2$  there are infinitely many non-isomorphic curves  $X$  over  $k$  with different two-part of the group of  $k$ -rational points on the Jacobian varieties associated to them.*

*Proof.* For any positive integer  $n$  there exists a monic irreducible polynomial of degree  $n$  with coefficients in  $\mathbb{F}_q$ . Let us pick any sequence of such polynomials  $D_n(x)$ ,  $n \in \mathbb{N}$  with the property that  $\deg(D_{n+1}(x)) > \deg(D_n(x))$  and  $\deg(D_1(x)) \geq 3$ . Consider the family of affine curves defined by the equation  $C_m : y^2 = D_1(x)D_2(x) \dots D_m(x)$ . Since  $D_i$ ,  $i \in \mathbb{N}$  are mutually distinct these affine curves are smooth. Let  $X_m$  denotes the normalization of the projective closure of  $C_m$ . Then  $X_m$  is a hyper-elliptic curve of the genus  $g_m = \lfloor \frac{\deg(D_1(x)) + \dots + \deg(D_m(x)) - 1}{2} \rfloor$ . The Weil-bound insures that the order of the group of  $\mathbb{F}_q$ -rational points of the Jacobian variety  $J_m$  associated to  $X_m$  satisfies the following:

$$(\sqrt{q} - 1)^{2g_m} \leq \#J_m(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g_m},$$

and therefore the two-part of  $J_m(\mathbb{F}_q)$  is bounded from above by  $(\sqrt{q} + 1)^{2g_m}$ . On the other hand theorem 1.4 from [3] states that the two-rank of  $J_m(\mathbb{F}_q)$  is at least  $m - 2$ . Therefore, among the family  $X_m$  there are infinitely many curves with different two-part of the group  $J_m(\mathbb{F}_q)$  and therefore their function fields  $K_m$  have non-isomorphic  $\mathcal{G}_{K_m}^{ab}$ .  $\square$



## References

- [1] Athanasios Angelakis and Peter Stevenhagen. Imaginary quadratic fields with isomorphic abelian Galois groups. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 21–39. Math. Sci. Publ., Berkeley, CA, 2013.
- [2] Emil Artin and John Tate. *Class field theory*. AMS Chelsea Publishing, Providence, RI, 2009. Reprinted with corrections from the 1967 original.
- [3] Gunther Cornelissen. Two-torsion in the jacobian of hyperelliptic curves over finite fields. *Archiv der Mathematik*, 77(3):241–246, 2001.
- [4] László Fuchs. *Abelian groups*. Springer Monographs in Mathematics. Springer, Cham, 2015.
- [5] Irving Kaplansky. *Infinite abelian groups*. Revised edition. The University of Michigan Press, Ann Arbor, Mich., 1969.
- [6] James R. C. Leitzel, Manohar L. Madan, and Clifford S. Queen. Algebraic function fields with small class number. *J. Number Theory*, 7:11–27, 1975.
- [7] Sidney A. Morris. *Pontryagin duality and the structure of locally compact abelian groups*. Cambridge University Press, Cambridge-New York-Melbourne, 1977. London Mathematical Society Lecture Note Series, No. 29.
- [8] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
- [9] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
- [10] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.
- [11] Kôji Uchida. Isomorphisms of Galois groups of algebraic function fields. *Ann. of Math. (2)*, 106(3):589–598, 1977.
- [12] André Weil. *Basic number theory*. Classics in Mathematics. Springer-Verlag, Berlin, 1995. Reprint of the second (1973) edition.

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Outline of the Proof</b>	<b>4</b>
<b>3</b>	<b>Proof of Lemmas</b>	<b>8</b>
3.1	Preliminaries . . . . .	8
3.1.1	The Pontryagin Duality . . . . .	9
3.2	Class Field Theory . . . . .	10
3.3	Deriving the main exact sequence . . . . .	11
3.4	On the Structure of the Kernel . . . . .	12
3.4.1	Description of $\mathcal{T}_q$ . . . . .	13
3.5	On the torsion of $\mathcal{C}_K^0$ . . . . .	18
3.6	Proof of the inverse implication . . . . .	18
3.6.1	The $p$ -part . . . . .	18
3.6.2	The non $p$ -part . . . . .	19
3.6.3	Proof of the Theorem 5 . . . . .	21
<b>4</b>	<b>Proof of Corollaries</b>	<b>24</b>